IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: **ATKINS ET AL.**	§	Attorney Docket No.:	**RPS920000026US1**
Serial No.: **09/651,548**	§	Examiner:	**SHIN, KYUNG H.**
Filed: **AUGUST 29, 2000**	§		
Title: **SYSTEM, METHOD AND PROGRAM FOR MANAGING A USER KEY USED TO SIGN A MESSAGE FOR A DATA PROCESSING SYSTEM**	§	Group Art Unit:	**2143**
	§	Confirmation No:	**9903**

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the appeal in the above-referenced application. Appellants have submitted the fee for the filing of an appeal brief herewith. If additional fees are required, please charge **Lenovo Inc. Deposit Account No. 50-3533**.

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is Lenovo Inc., the Assignee of the present application.

RELATED APPEALS AND INTERFERENCES

The present appeal is related to the earlier appeal of the present application, which resulted in a decision for Appeal No. 2006-2482 of the Board of Patent Appeals and Interferences mailed April 5, 2007, which reversed the final rejection of each pending claim. There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending Appeal.

STATUS OF CLAIMS

Claims 1-24 were originally presented. In Appellants' Amendment A, filed May 18, 2004, Claims 1, 3, 6-7, 9, 11, 14-15, 17, 19 and 23 were amended. Claims 1, 9 and 17 were also amended in Amendment C, filed October 9, 2007, and again in Amendment D, filed April 8, 2008. Claim 17 was further amended in Amendment E, filed September 4, 2008. No claims were canceled or entered during prosecution. Claims 1-24, which comprise all pending claims, stand finally rejected by the Examiner as noted in the Final Office Action dated December 24, 2008. The rejection of each of Claims 1-24 is appealed.

STATUS OF AMENDMENTS

No amendments to the claims have been proposed or entered subsequent to the final rejection that led to this appeal.

SUMMARY OF THE CLAIMED INVENTIONS

The invention recited in independent Claim 1 provides a method for managing a user key used to sign an electronic message. As depicted in step 304 of Figure 3 and described at page 14, lines 1-4, the method includes assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages. The encrypting data processing system can then encrypt messages with the user key, as depicted in step 306 of Figure 3 and as

described at page 14, lines 7-9. According to the claimed method, an associated key is also stored in the encrypting data processing system and used to encrypt to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27. The encrypting data processing system communicates at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15. Thereafter, validation of the association of the user with messages can be prevented by revoking the associated key at the encrypting data processing system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

In addition to the features of Claim 1, dependent Claim 3 recites that the encrypting data processing system further includes a client system and a server system coupled for communication (see, e.g., Figure 1, client systems 102A-102C and server system 104; page 9, lines 1-5), where the client system has a client memory device (see, e.g., Figure 1, memory system 103; page 9, lines 12-14) and the server system has an encryption chip and a server memory device (see, e.g., Figure 1, encryption chip 106 and memory device 105; page 9, lines 24-26). In addition, Claim 3 further recites that storing the user key further comprises storing the user key in the client memory device (see, e.g., Figure 1; page 10, lines 10-11), storing the associated key further comprises storing the associated key in the server memory device (see, e.g., Figure 1; page 10, lines 21-29), and preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device (see, e.g., Figure 3, block 320; page 15, lines 17-28).

In addition to the features recited in Claims 1 and 3, Claim 4 recites that encrypting the messages further comprises sending the messages to be encrypted from the client system to the server system (see, e.g., Figure 3, block 308; page 14, lines 11-22), encrypting the messages using the encryption chip of the server system (see, e.g., Figure 3, block 310; page 14, lines 24-29), and sending the encrypted messages from the server system to the client system (see, e.g., Figure 3, block 314; page 14, lines 29-32).

In addition to the features recited in Claim 1, Claim 6 recites encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system (see, e.g., Figure 3, block 312; page 14, lines 27-29).

In addition to the features recited in Claims 1 and 6, Claim 7 recites communicating an encrypted associated key to validate the association of the user with the encrypted messages (see, e.g., Figure 3, block 318; page 15, lines 4-15).

In addition to the features of Claims 1, 6 and 7, Claim 8 recites decrypting the associated key with the encryption chip key (see, e.g., Figure 4, block 408; page 16, lines 13-16).

The invention recited in independent Claim 9 provides a system for managing a user key used to sign an electronic message. Each of the elements of the system recited in Claim 9 is set forth in the means-plus-function format permitted by 35 U.S.C. § 112, paragraph 6. An exemplary data processing system 100 embodying the claimed system includes means for assigning a user key to a user (e.g., server system 104 of Figure 1), which assigns a user key to a user as depicted in step 304 of Figure 3 and described at page 14, lines 1-4. Data processing system 100 further includes means for storing a user key 103a, 103b, 103c, such hard disks 19, 29 of Figure 2. Data processing system 100 also includes means for encrypting the messages with the user key (e.g., encryption chip 106), as depicted in step 306 of Figure 3 and as described at page 14, lines 7-9. As depicted at reference numeral 120 of Figure 1, data processing system 100 also includes protected storage that serves as a means for storing an associated key (e.g., key A, key B, key C). Encryption chip 106 of data processing system 100 of Figure 1 further serves as a means for encrypting the user key with the associated key to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27. Data processing system 100 also includes means for communicating at least one encrypted message together with the encrypted user key to a recipient system (e.g., LAN interface 16 of Figure 2) in order to permit validation of an association of the user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15. Data processing system 100 further includes means (e.g., encryption chip 106) for thereafter preventing

validation of the association of the user with messages by revoking the associated key in the system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

In addition to the features of Claim 9, Claim 11 recites that the system further comprises a client system and a server system coupled together for communication (see, e.g., Figure 1, client systems 102A-102C and server system 104; page 9, lines 1-5), where the client system has a client memory device (see, e.g., Figure 1, memory system 103; page 9, lines 12-14) and the server system having an encryption chip and a server memory device (see, e.g., Figure 1, encryption chip 106 and memory device 105; page 9, lines 24-26). Claim 11 further recites, in the manner permitted by 35 U.S.C. § 112, sixth paragraph, that the means for storing the user key further comprises means for storing the user key in the client memory device (see, e.g., Figure 1; page 10, lines 10-11), the means for storing the associated key further comprises means for storing the associated key in the server memory device (see, e.g., Figure 1; page 10, lines 21-29), and the means for preventing validation further comprises means for preventing the validation of messages associated with the user by eliminating the associated key from the server memory device (see, e.g., Figure 3, block 320; page 15, lines 17-28).

In addition to the features of Claims 9 and 11, Claim 12 recites, in the manner permitted by 35 U.S.C. § 112, sixth paragraph, that the means for encrypting the messages further comprises means for sending the messages to be encrypted from the client system to the server system (see, e.g., Figure 3, block 308; page 14, lines 11-22), means for encrypting the messages using the encryption chip of the server system (see, e.g., Figure 3, block 310; page 14, lines 24-29), and means for sending the encrypted messages from the server system to the client system (see, e.g., Figure 3, block 314; page 14, lines 29-32).

In addition to the features of Claim 9, Claim 14 recites an encryption chip that encrypts the associated key by using an encryption chip key stored within the encryption chip (see, e.g., Figure 3, block 312; page 14, lines 27-29).

Dependent Claim 15 recites in the means-plus-function format provided for in 35 U.S.C. § 112, paragraph 6, a system for managing a user key used to sign an electronic message. Claim

15, which depends on Claim 13, recites, in addition to the features of Claim 13, means (e.g., client system 102 and its LAN interface 16) for communicating an encrypted associated key to validate the association of the user with the encrypted messages, as described at page 15, lines 4-15 and depicted in Figure 3 at block 318.

In addition to the features of Claims 9, 14 and 15, Claim 16 recites, in the manner permitted by 35 U.S.C. § 112, sixth paragraph, means for decrypting the associated key with the encryption chip key (see, e.g., Figure 4, block 408; page 16, lines 13-16).

The invention recited in independent Claim 17 provides a program product for managing a user key used to sign a message. The program product includes a control program (method 300 of Figure 3; page 13, lines 15-19) and a computer usable media bearing the control program (e.g., hard disks 19, 29 of Figure 2). Each of the elements of the control program recited in Claim 17 is set forth in the means-plus-function format permitted by 35 U.S.C. § 112, paragraph 6. These elements include instruction means for assigning a user key to a user and for storing the user key in an encrypting data processing system utilized to encrypt messages, as depicted in step 304 of Figure 3 and described at page 14, lines 1-4; instruction means for encrypting the messages with the user key, as depicted in step 306 of Figure 3 and as described at page 14, lines 7-9; instruction means for storing an associated key in the encrypting data processing system and for encrypting the user key with the associated key to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27; instruction means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15; and instruction means for thereafter preventing validation of the association of the user with messages by revoking the associated key within the encrypting data processing system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

In addition to the features of Claim 17, Claim 19 recites that the encrypting data processing system further comprises a client system and a server system coupled together for communication (see, e.g., Figure 1, client systems 102A-102C and server system 104; page 9,

lines 1-5), where the client system has a client memory device (see, e.g., Figure 1, memory system 103; page 9, lines 12-14) and the server system having an encryption chip and a server memory device (see, e.g., Figure 1, encryption chip 106 and memory device 105; page 9, lines 24-26). Claim 19 further recites that the instruction means for storing the user key further comprises instruction means for storing the user key in the client memory device (see, e.g., Figure 1; page 10, lines 10-11), the instruction means for storing the associated key further comprises instruction means for storing the associated key in the server memory device (see, e.g., Figure 1; page 10, lines 21-29), and the instruction means for preventing validation further comprises instruction means for preventing the validation of the messages associated with the user by eliminating the associated key from the server memory device (see, e.g., Figure 3, block 320; page 15, lines 17-28).

In addition to the features of Claims 17 and 19, Claim 20 recites, in the manner permitted by 35 U.S.C. § 112, second paragraph, that the instruction means for encrypting the messages further comprises instruction means for sending the messages to be encrypted from the client system to the server system (see, e.g., Figure 3, block 308; page 14, lines 11-22), instruction means for encrypting the messages using the encryption chip of the server system (see, e.g., Figure 3, block 310; page 14, lines 24-29), and instruction means for sending the encrypted messages from the server system to the client system (see, e.g., Figure 3, block 314; page 14, lines 29-32).

In addition to the features of Claim 17, Claim 22 recites, in the manner permitted by 35 U.S.C. § 112, sixth paragraph, instruction means for encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the data processing system (see, e.g., Figure 3, block 312; page 14, lines 27-29).

Dependent Claim 23 recites in the means-plus-function format provided for in 35 U.S.C. § 112, paragraph 6, a program product for managing a user key used to sign an electronic message. Claim 23, which depends on Claim 17, recites, in addition to the features of Claim 17, instruction means (e.g., method 300 of Figure 3; page 13, lines 15-19) for communicating an

encrypted associated key to validate the association of the user with the encrypted messages, as described at page 15, lines 4-15 and depicted in Figure 3 at block 318.

In addition to the features of Claims 17, 22 and 23, Claim 24recites, in the manner permitted by 35 U.S.C. § 112, sixth paragraph, instruction means for decrypting the associated key with the encryption chip key (see, e.g., Figure 4, block 408; page 16, lines 13-16).

GROUNDS OF REJECTION

The present Appeal is filed in response to the Final Office Action dated December 24, 2008, in which the following rejections are made:

(I) Claims 17-24 are rejected under 35 U.S.C. § 101 as non-statutory;

(II) Claims 1-4, 6-12, 14-20 and 22-24 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,807,277 to *Doonan et al.* (*Doonan*) in view of U.S. Patent No. 6,732,101 to *Cook*;

(III) Claims 5, 13 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Cook* in view of U.S. Patent No. 4,888,800 to *Marshall*.

ARGUMENT

I. Rejection of Claims 17-24 under 35 U.S.C. § 101

Claims 17-24 stand finally rejected under 35 U.S.C. § 101 as non-statutory. In particular, paragraph 4 of the Final Office Action states that Claims 17-24 are non-statutory because "there is no indication that the computer readable medium is in a state of execution and therefore is directed towards non-statutory subject matter." That rejection is not well-founded and should be reversed.

Appellants respectfully point out that the Examiner's rejection is founded upon a requirement (viz. "there is no indication that the computer readable medium is in a state of execution") not found in 35 U.S.C. § 101, the Manual of Patent Examining Procedure (MPEP) or the case law of the Supreme Court and Federal Circuit. With reference to computer-related inventions, MPEP 2106.01 states:

> Computer programs are often recited as part of a claim. USPTO personnel should determine whether the computer program is being claimed as part of an otherwise statutory manufacture or machine. In such a case, the claim remains statutory irrespective of the fact that a computer program is included in the claim. The same result occurs when a computer program is used in a computerized process where the computer executes the instructions set forth in the computer program. Only when the claimed invention taken as a whole is directed to a mere program listing, i.e., to only its description or expression, is it descriptive material *per se* and hence nonstatutory.
>
> Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and USPTO personnel should treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material. When a computer program is claimed in a process where the computer is executing the computer program's instructions, USPTO personnel should treat the claim as a process claim. ** When a computer program is recited in conjunction with a physical structure, such as a computer memory, USPTO personnel should treat the claim as a product claim. [Emphasis supplied]

Thus, MPEP 2106.01 mandates recitation of a "state of execution" as urged by the Examiner for process claims only, thus prohibiting an applicant from claiming method steps amounting to a mere program listing (e.g., providing a first instruction, providing a second instruction, etc.). For claims, such as exemplary Claim 17, which recite an article of manufacture, MPEP 2106.01 further states that "[w]hen a computer program is recited in conjunction with a physical structure, such as a computer memory, USPTO personnel should treat the claim as a product claim" and thus statutory under 35 U.S.C. § 101.

Further, the Examiner has failed to interpret the means-plus-function language of exemplary Claim 17 and its dependent claims as demanded by Federal Circuit precedent and MPEP 2106. As stated in MPEP 2106 with reference to rejections under 35 U.S.C. § 101:

> Where means plus function language is used to define the characteristics of a machine or manufacture invention, **such language must be interpreted** to read on only the structures or materials disclosed in the specification and "equivalents thereof" that correspond to the recited function. Two *en banc* decisions of the Federal Circuit have made clear that the USPTO is to interpret means plus function language according to 35 U.S.C. § 112, sixth paragraph. *In re Donaldson*, 16 F.3d 1189, 1193, 29 USPQ2d 1845, 1848 (Fed. Cir. 1994) (*en*

banc); *In re Alappat*, 33 F.3d 1526, 1540, 31 USPQ2d 1545, 1554 (Fed. Cir. 1994) (*en banc*). [Emphasis supplied]

In the present case, the Examiner has failed to interpret exemplary Claim 17 and its dependent claims as required by the holdings in *In re Donaldson* and *In re Alappat* and MPEP 2106. For this reason alone, it is clear that the rejection under 35 U.S.C. § 101 is not well founded and should be reversed.

Had the Examiner comported with the requirement to interpret exemplary Claim 17 and its dependent claims in accordance the holdings in *In re Donaldson* and *In re Alappat* and MPEP 2106, the Examiner would have to construe the recited "instruction means for ..." of exemplary Claim 17, *inter alia*, by reference to page 17, line 34 through page 18, line 10 of the present specification, which discloses "signal-bearing media, when carrying or encoding computer readable instructions that direct the functions of the present invention, represent alternative embodiments of the present invention" (emphasis supplied). Hence, it is clear that the recited "instructions means for ..." recited in exemplary Claim 17 and its dependent claims are not mere non-statutory nonfunctional descriptive material (i.e., a mere program listing), but instead are "functional descriptive material," as that term is employed in MPEP 2106.01.

In particular, MPEP 2106.01 states in relevant part:

> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. ... "Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data.
>
> Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. [Citations omitted; emphasis supplied]

In the present case, the functional descriptive material of exemplary Claim 17, which resides in "a computer usable storage medium storing said control program" is clearly statutory "since use of technology permits the function of the descriptive material to be realized" as stated in MPEP

2106.01. Appellants therefore respectfully request reversal of the rejection of Claims 17-24 under 35 U.S.C. § 101.

II. Rejection of Claims 1-4, 6-12, 14-20 and 22-24 under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Cook*

A. Exemplary independent Claim 1

1. Combination of *Doonan* and *Cook* does not disclose the claimed step of "storing an associated key in the encrypting data processing system and encrypting the user key with the associated key ..." as recited in Claim 1

The combination of *Doonan* and *Cook* does not render exemplary Claim 1 (and similar Claims 9 and 17) of the present invention unpatentable under 35 U.S.C. § 103 because the combination of cited references does not disclose each feature recited therein. For example, the combination of *Doonan* and *Cook* does not disclose the following step of exemplary Claim 1:

> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key.

With respect to the claimed "associated key", page 6 of the Final Office Action first cites col. 5, lines 63-67 of *Doonan*, which disclose:

> The composite message P is first encrypted to form encrypted message Pe, using a randomly-generated symmetric encryption key Ks. The symmetric key Ks is then itself encrypted using the public key published in a digital certificate owned by the recipient, to form [the encrypted symmetric key] Kp. (emphasis supplied)

Thus, *Doonan's* public key of the message recipient is relied upon in the present rejection as disclosing the claimed "associated key." However, Claim 1 explicitly recites that the "associated key comprises a private key," rather than a public key as disclosed by *Doonan*.

In recognition of the failure of *Doonan* to disclose the encryption of the user key with a private associated key as claimed, page 6 of the Final Office Action notes that col. 5, lines 48-50 of *Doonan* further disclose the encryption of the hash of a message with a private key to obtain a digital signature. However, there is no objective evidence of record that a person of ordinary skill in the art would be led to modify the explicit teaching of the combination of *Doonan* and

Cook (i.e., encrypting a symmetric key with a public key to obtain an encrypted key) to obtain the claimed step of encrypting a user key with a private associated key to obtain an encrypted user key based upon *Doonan's* further disclosure of encrypting a hash of a message (rather than a user key as claimed).

The Examiner's modification to the reference teachings is also not obvious to the ordinarily skilled artisan because it renders the prior art unsatisfactory for its intended purpose and changes its principle of operation, in contravention of MPEP 2143.01. As made clear by MPEP 2143.01:

> If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)
> ...
> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

In the present case, the Examiner blithely suggests substitution of a private key of the sender in place of the public key of the recipient of a message. If this operation were performed as suggested by the Examiner, then the recipient of the message would be unable to decrypt the encrypted symmetric key needed to decrypt the message, as disclosed, for example, at block 708 of Figure 7 and col. 7, lines 3-16 of *Doonan*, as this step requires the recipient to be able to perform the decryption using the recipient's private key corresponding to the public key with which the symmetric key was encrypted. Thus, the modification suggested by the Examiner represents a significant change in the principle of operation of *Doonan* and *Cook* and would render the disclosed encryption process unsatisfactory for its intended purpose.

In view of the foregoing, it is evident that the combination of *Doonan* and *Cook* does not disclose or render obvious each feature of exemplary Claim 1 and therefore does not render Claims 1, 9 and 17 and their respective dependent claims unpatentable under 35 U.S.C. § 103.

2. Combination of *Doonan* and *Cook* does not disclose the claimed step of "preventing validation ..." as recited in Claim 1

Applicant further respectfully submits that the combination of *Doonan* and *Cook* does not render exemplary Claim 1 unpatentable under 35 U.S.C. § 103 because that combination of references does not disclose the following step of exemplary Claim 1 as amended:

> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key. [Emphasis supplied]

With reference to the step of "preventing validation of the association of the user with messages," pages 6-7 of the Final Office Action correctly note that *Doonan* does not disclose revocation of an associated key as claimed. However, the Office Action then relies upon *Cook's* disclosure of the conventional deletion of a key by a signature manager 132 at col. 6, lines 40-50:

> Signature manager 132 is a utility for managing encryption keys for a user. Prior to the use of wrapping application 128 or viewer 130, each user (e.g., sender 102 or fully configured recipient 104a) must generate public and private keys. Signature manager 132 includes methods for generating public and private keys. Signature manager 132 submits the public key to key server 108 for publication. Key server 108 publishes the public keys in a key list which in turn can be distributed to key retrieval servers 180. Signature manager 132 can be used to create new keys, change keys, delete keys or change signature phrases. [Emphasis supplied]

The combination of *Doonan* and *Cook* urged by the Examiner thus requires a signature manager 132 at the encrypting (i.e., sender) data processing system to delete the public key of a message recipient. As should be apparent, the simple deletion at the sender (i.e., encrypting) system of a message recipient's public key does not "prevent[ ] validation of the association of the user with messages" and does not render the encrypting data processing system unable "to decrypt the encrypted user key" as claimed. Instead, a user of the sender system can easily again access the recipient's public key at any time utilizing *Cook's* key retrieval server 180, as taught by *Cook* at col. 6, lines 40-50, and thereby again access the encrypted user key. Thus, the

combination of *Doonan* and *Cook* does not render obvious the claimed step of "preventing validation of the association of the user with messages" recited in exemplary Claim 1.

The Examiner attempts to respond to Appellants' argument at page 3 of the Final Office Action by noting that Appellant's specification teaches that an associated key "may be revoked by simply erasing it" and states that this is merely the key deletion disclosed by *Cook*. In response, Appellants respectfully submit that the Examiner has missed the point entirely. The Examiner is focused on *how* key revocation is performed (i.e., by deleting the key) rather than *which* key is revoked. In exemplary Claim 1, a private associated key is revoked at the encrypting data processing system. In the Examiner's combination of *Doonan* and *Cook*, a public key of the message recipient is revoked, which does not meet the claimed feature that "the encrypting data processing system is no longer able to decrypt the encrypted user key." Consequently, the combination of *Doonan* and *Cook* does not disclose or render obvious each feature of exemplary Claim 1 and therefore does not render Claims 1, 9 and 17 and their respective dependent claims unpatentable under 35 U.S.C. § 103.

B. Exemplary dependent Claims 3-4, 11-12 and 19-20

The combination of *Doonan* and *Cook* also fails to render Claims 3-4, 11-12, and 19-20 unpatentable under 35 U.S.C. § 103 because the cited combination of references does not disclose "said server system having an encryption chip" as recited in exemplary Claim 3 (and similarly in Claims 11 and 19) or "encrypting the messages using the encryption chip of the server system" as recited in exemplary Claim 4 (and similarly in Claims 12 and 20).

In the rejection of exemplary Claim 3, the Examiner does not indicate where the combination of cited references discloses the claimed encryption chip. Similarly, in the rejection of exemplary Claim 4, the Examiner cites col. 2, lines 51-55 of *Cook* as generally disclosing the encryption of an email message, but fails to indicate where the combination of references discloses the claimed encryption chip. Consequently, it is apparent that the Examiner has not established a *prima facie* case of obviousness with respect to Claims 3-4, 11-12, and 19-20, and the rejection of Claims 3-4, 11-12, 19-20 (and their dependent claims) under 35 U.S.C. § 103 should be reversed.

C. Exemplary dependent Claims 6-8, 14-16 and 22-24

1. Combination of cited references does not disclose claimed "encryption chip"

The combination of *Doonan* and *Cook* also fails to render Claims 6-8, 14-16 and 22-24 unpatentable under 35 U.S.C. § 103 because the cited combination of references does not disclose the "encryption chip" recited in each of these claims, either directly or by virtue of dependency. Consequently, it is apparent that the Examiner has not established a *prima facie* case of obviousness with respect to Claims 6-8, 14-16 and 22-24, and the rejection of Claims 6-8, 14-16 and 22-24 under 35 U.S.C. § 103 should be reversed.

2. Combination of cited references does not disclose encrypting the associated key as recited in exemplary Claim 6

The combination of *Doonan* and *Cook* also fails to render exemplary Claim 6, similar Claims 14 and 22, and their respective dependent Claims 7-8, 25-26 and 23-24 unpatentable under 35 U.S.C. § 103 because the cited combination of references does not disclose encrypting the associated key as recited in exemplary Claim 6 as follows:

> encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system.

With reference to the foregoing step, page 10 of the present Office Action cites col. 2, lines 3-8 of *Doonan*, which discloses:

> The Key Server generates an [sic] pair of message keys, stores a copy of the decryption key, and returns the encryption key to the sender along with some information that can be used to retrieve the decryption key at a later time. The sender uses the encryption key to encrypt the message contents.

It should be apparent that the cited passage of *Doonan* does not disclose "encrypting the associated key" or doing so with an "encryption chip key which is stored on an encryption chip," as claimed. Consequently, the combination of cited references does not disclose the features recited in exemplary Claim 6, and the rejection of Claims 6-8, 14-16 and 22-24 under 35 U.S.C. § 103 should be reversed.

III. Rejection of Claims 5, 13 and 21 under 35 U.S.C. § 103 as unpatentable over *Doonan*, *Cook* and *Marshall*

The combination of *Doonan* and *Cook* also fails to render Claims 5, 13 and 21 unpatentable under 35 U.S.C. § 103 for at least the reasons set forth above with reference to exemplary Claims 1 and 4. Accordingly, the rejection of dependent Claims 5, 13 and 21 under 35 U.S.C. § 103 should be reversed.

IV. Conclusion

The foregoing remarks demonstrate that the combination of cited references does not disclose or render obvious each feature of Claims 1-24 as required to support a rejection under 35 U.S.C. § 103. Appellants therefore respectfully request the Board to reverse the final rejection of each of Claims 1-24.

Respectfully submitted,

Brian F. Russell
Reg. No. 40,796
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
(512) 343-6116
ATTORNEY FOR APPELLANTS

APPENDIX A
CURRENTLY PENDING CLAIMS

1. A method for managing a user key used to sign a message for a data processing system, said method comprising:

assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;

encrypting the messages with the user key;

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key;

said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key.

2. The method according to Claim 1, further comprising:

decrypting the user key with the associated key; and

decrypting the messages with the user key.

3. The method according to Claim 1, wherein:

the encrypting data processing system further comprises a client system and a server system coupled for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

storing the user key further comprises storing the user key in the client memory device;

storing the associated key further comprises storing the associated key in the server memory device; and

preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

4. The method according to Claim 3, wherein encrypting the messages further comprises:

sending the messages to be encrypted from the client system to the server system;

encrypting the messages using the encryption chip of the server system; and

sending the encrypted messages from the server system to the client system.

5. The method according to Claim 4, further comprising:

erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

6. The method according to Claim 1, further comprising:

encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system.

7. The method according to Claim 6, further comprising:

communicating an encrypted associated key to validate the association of the user with the encrypted messages.

8. The method according to Claim 7, further comprising:

decrypting the associated key with the encryption chip key.

9. A system for managing a user key used to sign a message, said system comprising:

means for assigning a user key to a user;

means for storing the user key;

means for encrypting the messages with the user key;

means for storing an associated key;

means for encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key;

means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

means for thereafter preventing validation of the association of the user with messages by revoking the associated key in said system so that the encrypting data processing system is no longer able to decrypt the encrypted user key.

10. The system according to Claim 9, further comprising:

means for decrypting the user key with the associated key; and

means for decrypting the messages with the user key.

11. The system according to Claim 9, wherein:

the system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

said means for storing the user key further comprises means for storing the user key in the client memory device;

said means for storing the associated key further comprises means for storing the associated key in the server memory device; and

said means for preventing validation further comprises means for preventing the validation of messages associated with the user by eliminating the associated key from the server memory device.

12. The system according to Claim 11, wherein said means for encrypting the messages further comprises:

means for sending the messages to be encrypted from the client system to the server system;

means for encrypting the messages using the encryption chip of the server system; and

means for sending the encrypted messages from the server system to the client system.

13. The system according to Claim 12, further comprising:

means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

14. The system according to Claim 9, further comprising:

an encryption chip that encrypts the associated key by using an encryption chip key stored within the encryption chip.

15. The system according to Claim 14, further comprising:

means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.

16. The system according to Claim 15, further comprising:

means for decrypting the associated key with the encryption chip key.

17. A program product for managing a user key used to sign a message, said program product comprising:

a control program including:

instruction means for assigning a user key to a user and for storing the user key in an encrypting data processing system utilized to encrypt messages;

instruction means for encrypting the messages with the user key;

instruction means for storing an associated key in the encrypting data processing system and for encrypting the user key with the associated key to obtain an encrypted user key, wherein said associated key comprises a private key;

instruction means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system;

instruction means for thereafter preventing validation of the association of the user with messages by revoking the associated key within the encrypting data processing system so that the encrypting data processing system is no longer able to decrypt the encrypted user key; and

a computer usable storage medium storing said control program.

18. The program product according to Claim 17, further comprising:

instruction means for decrypting the user key with the associated key; and

instruction means for decrypting the messages with the user key.

19. The program product according to Claim 17, wherein:

the encrypting data processing system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

said instruction means for storing the user key further comprises instruction means for storing the user key in the client memory device;

said instruction means for storing the associated key further comprises instruction means for storing the associated key in the server memory device; and

said instruction means for preventing validation further comprises instruction means for preventing the validation of the messages associated with the user by eliminating the associated key from the server memory device.

20. The program product according to Claim 19, wherein said instruction means for encrypting the messages further comprises:

instruction means for sending the messages to be encrypted from the client system to the server system;

instruction means for encrypting the messages using the encryption chip of the server system; and

instruction means for sending the encrypted messages from the server system to the client system.

21. The program product according to Claim 20, further comprising:

instruction means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

22. The program product according to Claim 17, further comprising:

instruction means for encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the data processing system.

23. The program product according to Claim 22, further comprising:

instruction means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.

24. The program product according to Claim 23, further comprising:

instruction means for decrypting the associated key with the encryption chip key.

APPENDIX B
EVIDENCE APPENDIX

(none)

APPENDIX C
RELATED PROCEEDINGS APPENDIX

Appeal No. 2006-2482; Decision on Appeal mailed April 5, 2007

The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte BARRY ATKINS, DAVID CARROLL CHALLENER, FRANK NOVAK, JOSEPH GARY RUSNAK, KENNETH D. TIMMONS, and WILLIAM W. VETTER

Appeal 2006-2482
Application 09/651,548
Technology Center 2100

Decided: April 5, 2007

Before LANCE LEONARD BARRY, MAHSHID D. SAADAT, and JEAN R. HOMERE, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

(Reversed)

DECISION ON APPEAL

I. STATEMENT OF THE CASE

An Examiner rejected claims 1-24. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

A. THE INVENTION

The invention at issue on appeal concerns "cryptography." (Specification 1.) Cryptography involves encrypting data to provide security for the data. Before transmitting a message from one party to another, for example, a mathematical function known as a "cryptographic algorithm" is used to encrypt the message. (*Id.*) The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key," is required to decrypt an encrypted message. (*Id.*)

The Appellants opine that centralization of encryption and decryption at a server can lead to a problem in key management. More specifically, a client system is assigned a key provided to the user of the system. Various keys for various client systems are used and managed by the server. If the key issued for a particular client system needs to be revoked, the user may maintain a copy of the revoked key and thereby gain unlawful access to encrypted data. (*Id.* at 8.)

The Appellants assert that their invention consolidates the encryption and decryption in a centralized location while avoiding the aforementioned

problem. (*Id.*) A further understanding of the invention can be had by reading the following claim.

> 1. A method for managing a user key used to sign a message for a data processing system, said method comprising:
>
> assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;
>
> encrypting the messages with the user key;
>
> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;
>
> said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and
>
> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

B. THE REJECTIONS

Claims 1-3, 6-11, 14-19, and 22-24 stand rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,807,277 ("Doonan") and U.S. Patent No. 6,009,177 ("Sudia"). Claims 4, 12, and 20 stand rejected under

§ 103(a) as obvious over Doonan, Sudia, and U.S. Patent No. 6,732,101 ("Cook"). Claims 5, 13, and 21 stand rejected under § 103(a) as obvious over Doonan, Sudia, Cook, and U.S. Patent No. 4,888,800 ("Marshall").

II. ISSUE

Rather than reiterate the positions of parties *in toto*, we focus on an issue therebetween. The Examiner admits, "Doonan does not specifically disclose using a certificate authority (trusted third party) for key validation and determination of key revocation," (Answer 4-5.), and "Doonan does not specifically disclose a usage of encryption key pairs and to revoke an encryption key pair." (*Id.* at 11.) The Examiner asserts, however, "Sudia discloses preventing validation of the association of the user with messages by revoking the associated key at the encryption data processing system (see Sudia col. 22, lines 51-63, col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)[.]" (*Id.* at 5.) Appellants argue that "the conventional publication of the recipient's public key on a CRL as taught by *Doonan* and *Sudia* does not revoke the public key 'at' the encrypting data processing system. . . ." (Br. 7.) Therefore, the issue is whether the prior art would appear to have suggested require encrypting system to revoke a key stored therein.

In addressing the issue, the Board conducts a two-step analysis. First, we construe the independent claims at issue to determine their scope.

Second, we determine whether the construed claims would have been obvious.

III. CLAIM CONSTRUCTION

"Analysis begins with a key legal question — what is the invention claimed?" *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1567, 1 USPQ2d 1593, 1597 (Fed. Cir. 1987). In answering the question, "the PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324, 72 USPQ2d 1209, 1210-11 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1668 (Fed. Cir. 2000)).

Here, independent claim 1 recites in pertinent part the following limitations:

> assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;
>
> storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;
>
> thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

Independent claims 9 and 17 recite similar limitations. Giving the independent claims the broadest, reasonable construction, the limitations require an encrypting system to revoke a key stored therein.

IV. OBVIOUSNESS DETERMINATION

"Having determined what subject matter is being claimed, the next inquiry is whether the subject matter would have been obvious." *Ex Parte Massingill*, No. 2003-0506, 2004 WL 1646421, at *3 (B.P.A.I 2004). "In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "'A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art.'" *In re Bell*, 991 F.2d 781, 783, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

Here, Sudia explains that "[a] user who desires to send an encrypted communication to another user must have an escrow certificate for his own device and an escrow certificate for the intended recipient's public encryption key, because the device of the [the reference's] invention will neither encrypt

nor decrypt if either is missing." (Col. 21, ll. 15-20.) "[B]ecause the sender's device will not encrypt and the recipient's device will not decrypt unless the recipient's public encryption key certificate is 'valid,'" (*id.* at ll. 28-30), the device must first "verify the properties of the recipient's public encryption key certificate or of the digital signatures thereon. . . ." (*Id.* at ll. 57-58.)

The first part of Sudia cited by the Examiner discloses that "[w]henever any user, entity or device 'verifies' a digitally signed 'certificate,'" (col. 22, ll. 51-52.), the former "checks any applicable 'certificate revocation list' ('CRL') . . . to determine whether the certifying authority or other issuer has distributed, propagated or otherwise made available a list of revoked certificates . . . and whether, based upon the issuer name and certificate number, the certificate has been revoked." (*Id.* at ll. 57-63.) We find no teaching or suggestion in this part of the reference, nor the other part cited by the Examiner, however, that an encrypting user, entity, or device revokes a certificate or an intended recipient's public encryption key. To the contrary, we agree with Appellants that "[s]uch revocation can be said to be made 'at' the certifying authority that publishes the CRL. . . ." (Br. 7.)

In the *Response to Argument* section of his Answer, the Examiner refers to Cook for evidence of "the capability to revoke an association key pair by deleting an association encryption key pair." (Answer 12.) "Where a reference is relied on to support a rejection, whether

REVERSED

kis/gw

DILLON & YUDELL, LLP
8911 NORTH CAPITAL OF TEXAS HWY, SUITE 2100
AUSTIN, TX 78759